

**AFFIDAVIT
of
ANDREW EVANS
DETECTIVE
BOONE COUNTY SHERIFF'S OFFICE**

I, Andrew Evans, being first duly sworn, do depose and state that:

INTRODUCTION AND AGENT BACKGROUND

1. I am a federally deputized Detective, with the Boone County Sheriff's Office, and am assigned to the Cyber Crimes Task Force in Columbia, Missouri. Over my 20-year-career I have thousands of hours of certified law enforcement training. I was assigned to the Task Force in 2014 and hold several hundred hours in the investigation and exploitation of children through the Internet. I have participated in numerous investigations concerning violations of Title 18, United States Code. I have gained expertise in the conduct of such investigations through training in seminars, trainings, and everyday work related to these types of investigations. I have personally led multiple investigations involving the exploitation of children.

PROPERTY TO BE SEARCHED

2. I am investigating violations of Title 18, United States Code, Sections 2251, 2252 and 2256, certain activities relating to material involving the sexual exploitation of minors, in the Western District of Missouri. This affidavit is made in support of an application for a warrant to search the premises located at 5007 Willowby Drive, Jefferson City, Cole County, Missouri, which is more particularly described in Attachment A ("Target Premises"). Additionally, this application is to search any computer, smart phone, and computer media found therein, as specified in Attachment B, and to seize all items listed in Attachment B as contraband, instrumentalities, and evidence of crime.

PROBABLE CAUSE

3. This affidavit is based upon information I have gained from my investigation, my training and experience, as well as information obtained from conversations with other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2251, 2252 and 2256, are located at the target premises. Based upon the following information, there is probable cause to believe that currently located within the above-described premises is the evidence, fruits and instrumentalities of knowingly transferring visual depictions of minors engaged in sexually explicit conduct, in violation of Title 18, United States Code, Sections 2251, 2252 and 2256.
4. On Tuesday, May 21, 2024, I received a CyberTip from the National Center for Missing and Exploited Children, known as NCMEC, report # CT190083713. The National Center for Missing and Exploited Children operates a web-based reporting system that facilitates the reporting of Internet related crimes against children. NCMEC received information from Kik Inc. regarding Kik user “**daddydomdwolf**” had uploaded 38 videos to Kik’s infrastructure believed to be child sexual abuse material commonly referred to as CSAM. Kik provided the videos with the report. I viewed the videos which depicted multiple nude prepubescent male and female children approximately 1-8 years in age engaged in sexual conduct with adults as well as displayed in a lewd and lascivious manner by having their genitalia visible. One video specifically depicted a nude prepubescent female approximately 5 years of age blindfolded with her legs and hands in restraints while being vaginally

sodomized by and adult male.

5. Kik provided the following suspect information with the NCMEC report. An email address of speckhalsd.63@gmail.com was provided by the account creator at the time of account creation.
6. I used law enforcement data bases known to produce accurate results and searched the provided email address. One of those data bases was the Missouri State Highway Patrol Sex Offender Website. I located a person named Harold Dale Speckhals; a current Tier 1 sex offender required to register annually in Cole County, Missouri with a visually similar email address of dalespeckhals63.ds@gmail.com
7. I contacted the Cole County Sheriff's Office and spoke to Theresa Doggett. Theresa is employed by the Cole County Sheriff's Office as a support staff member and has access to Cole County sex offender registrations. Theresa confirmed Harold Dale Speckhals was a registered sex offender in Cole County currently listed as compliant. Theresa confirmed Harold's most recent sex offender registration which was signed and dated on July 27, 2023.
8. I reviewed Harold's sex offender registration and observed Harold had listed his personal email address as dalespeckhals63.ds@gmail.com. The email address listed for the suspect on the NCMEC report was speckhalsd.63@gmail.com. I observed Harold listed his current address as 5007 Willowby Drive, Jefferson City, Missouri. I observed Harold listed his current employment as Scholastic Inc located as 6325 Stertzer Road, Jefferson City, Cole County, Missouri. Harold also listed Kik as one of his registered social media accounts.
9. Furthermore, an IP address of 199.19.143.102 and 104.166.221.106 were captured on

when the reported videos were uploaded to Kik's infrastructure. Pursuant to a Boone County court order obtained on June 10th, 2024, I learned IP address 104.166.221.106 is registered to 5007 Willowby Drive, Jefferson City Missouri utilizing Mediacom Internet Services. This is the registered home address of Harold Dale Speckhals.

10. On May 24, 2024, I received information from Greg Denny an Internet Technology Specialist employed by Scholastics in Jefferson City, Missouri that IP address 199.19.143.102 was registered to Scholastic Inc. Per Greg Scholastic employees do have access to Scholastic provided Wi-Fi access while working. Per Harold's Sex Offender Registry; Harold was employed at Scholastics at the time of the reported CSAM uploads.
11. On May 31, 2024, I received additional data from Kik, Inc. pursuant to a previously obtained search warrant. I reviewed the data in its entirety. Kik provided data from June 25, 2023 through March 22, 2024. IP address 104.166.221.106 was captured approximately 6,300 times from 5007 Willowby Drive, Jefferson City, Missouri logging into, maintaining an IP connection an accessing the account containing CSAM. Scholastic IP address 199.19.143.102 was captured approximately 8,300 times connecting to, maintaining connection and or accessing the account reported for CSAM.
12. Also located within the Kik data were an additional 984 media files, of which 387 were videos that depicted nude prepubescent females between the approximate ages of 2 and 10, but some as young as infants engaged in sexual conduct with adults. Also seen in this data were multiple self-images of Harold Speckhals wearing lingerie and or being nude.
13. Furthermore, Kik provided both private and group platform message logs that indicated Harold disseminated approximately 2,877 media files to unknown users on the Kik platform many being CSAM media files.

14. Based on my training and experience data located within the Kik gallery section was consistent with individuals who share, trade and possess CSAM. Furthermore, based on the number of self-images seen of Harold in the data; I have probable cause to believe that registered sex offender Harold Dale Speckhals is the owner of the reported Kik account.
15. On February 1, 2001, Harold Dale Speckhals was convicted in Cole County Missouri, for Sexual Misconduct 1st Degree of a 14 year-old child RsMo 566.083 a Class D felony offense.
16. Missouri statute 589.414 states that any person adjudicated for a crime of sexual assault is a tier I sex offender and must register annually. Part of Harold's registration requirement falls under Missouri statute 589.407 which requires Harold to list any existing or new online identifiers when he registers. Harold failed to provide the following list of online identifiers at his most recent registration that occurred on July 23, 2023: **speckhalsd.63@gmail.com** and **daddydomdewolf**.
17. Using the Missouri Department of Revenue Website, I located a valid Missouri Driver's license for Harold Dale Speckhals. Harold's listed home address on his driver's license is 5007 Willowby Drive, Jefferson City, Missouri.

Definitions Use OF Computers With Child Exploitation

18. The development of computers and smart phones has added to the methods individuals use to interact with and sexually exploit children. Computers serve multiple functions in connection with child exploitation cases, such as production of images, communication, distribution of images, syncing of electronic devices and storage of images and communications.

19. With Internet access, a computer user can transport an image file from the Internet to another user's computer to his own computer, smart phone, or mobile device, so that the image file is stored in his computer, phone, or mobile device.
20. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only
21. overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.
22. The computer's capability to store images in digital form makes it an ideal repository for pornography. The size of the electronic storage media (commonly referred to as a hard

drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera or camera on a phone to capture an image, process that image in a computer with a video capture board, and to save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

23. Smart phone technology has expanded computer capability in recent years by allowing users to access the Internet via their phone. The smart phone user can search the Internet for specific files, check personal email accounts, log on to social networking sites, communicate with other computer users, compose and edit documents, produce photographic images, and store and view movie and picture files. Further, smart phone technology allows users to back the contents of their phone up to a computer and transfer image files from their smart phone to a computer or other electronic device.

The Internet And Technical Terms Pertaining To Computers

24. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive

information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail (“e-mail”). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet – for example, through a university, an employer, or a commercial service – which is called an “Internet Service Provider” or “ISP” (see definition of “Internet Service Provider” below). Once the individual has accessed the Internet, that individual can use Internet mail services, including sending and receiving e-mail. In addition, the individual can visit websites (see definition of “websites” below), and make purchases from them.

25. Set forth below are some definitions of technical terms, used throughout this Affidavit pertaining to the Internet and computers more generally:

- a. Computer system and related peripherals, and computer media: As used in this affidavit, the terms “computer system and related peripherals, and computer media” refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, smart phones, mobile devices in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.
- b. Internet Service Providers (ISPs) and the Storage of ISP Records: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their

customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and personal password. ISPs maintain records (“ISP records”) pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP’s servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers’ use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental

storage is defined by statute as “electronic storage,” see 18 U.S.C. § 2510(17), and the provider of such a service is an “electronic communications service.” An “electronic communications service,” as defined by statute, is “any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a “remote computing service.” 18 U.S.C. § 2711(2).

- c. Log File: Log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, log on/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

Specifics Of Search And Seizure Of Computer System

- 26. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that in order to completely and accurately retrieve data maintained in computer hardware or on computer software, all computer equipment, peripherals, related instructions in the form of manuals and notes, as well as the software utilized to operate such a computer, must be seized and subsequently processed by a qualified computer specialist in an appropriate setting such as an office or laboratory. This is true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.
 - b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even “hidden,” erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a “booby trap”), a controlled environment is essential to its complete and accurate analysis.
27. Based upon my consultation with experts in computer searches, data retrieval from computers, and related media and consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, I know that

searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

- a. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them in a reasonable time.
- b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as central processing unit (CPU). In cases like this one where the evidence consists partly of graphics files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system

software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

- c. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime of transmitting child pornography in violation of law and should all be seized as such.
- d. I am familiar with and understand the implications of the Privacy Protection Act (“PPA”), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the Target Premises are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

Method Of Searching And Examining Computers And Digital Evidence

28. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer

a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. *IP Address*: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term-IP addresses, while other computers have dynamic—that is, frequently changed-IP addresses.
 - c. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
29. Based on my training, experience, and research, I know that computers and smart phones have capabilities that allow it to serve as a device to facilitate communications via the Internet, and also retain files containing contraband, and other related documents and

communications, including email communications. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

30. I know from training and experience that most mobile device users protect access to their device contents via biometric methods. Biometric access includes but is not limited to fingerprint, iris, and facial recognition features. On many devices, biometric access is disabled once a device loses power, is restarted, or during other varying device processes, at which time a passcode or password is required. Due to the default encrypted state of most modern mobile devices, bypassing these security measures absent biometric access from the owner is not possible, thereby preventing a search of evidentiary data or forensic data extraction and analysis of device contents. This court grants permission to compel the owner of a mobile device or devices to provide biometric access to unlock device contents, if that item can be unlocked with biometric access. It is further ordered that should the owner refuse to comply with this order, investigators may compel by the use of reasonable force if necessary.

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. There is probable cause to believe that things that were once stored on the computer(s) and smart phone(s) may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

33. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.

34. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operations, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

35. *Forensic evidence.* As further described in the respective Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the computer(s) and smart phone(s) were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic

evidence might be on the items because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team

and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

36. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

37. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

38. Based upon the foregoing, I assert that probable cause exists that the computer, smart phone, computer media, and related documents pertaining to knowingly transferring visual depictions of minors engaged in sexually explicit conduct, in violation of Title 18, United States Code, Sections 2251, and 2252, are located on the premises at 5007 Willowby Drive, Jefferson City, Missouri.

39. The facts set forth in this affidavit are true and correct to the best of my knowledge and belief.

Andy Evans

Andy Evans

Federally Deputized Detective
Boone County Sheriff's Office

Attested to in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone or other reliable electronic means on this the 18th day of June 2024.

Willie J. Epps, Jr.

Willie J. Epps, Jr.

Chief United States Magistrate Judge

